

The Claims

1. (Currently amended) An installation module comprising:
an encrypted software module;
a decryption key to decrypt the encrypted software module; and
an executive for using the decryption key to ~~decrypting~~ the encrypted software module when at least one of a set of trigger files is stored on a computing system, wherein each of the trigger files indicates authorization to install the encrypted software module ~~consists of only content other than a decryption key for decrypting the encrypted software module.~~

2. (Currently amended) An installation module comprising:
an encrypted software module;
a key;
an executive for decrypting the encrypted software module with the key when at least one of a set of trigger files is stored on a computing system; and
a database for identifying the trigger files.

3. (Currently amended) The installation module of claim 2, wherein the database includes the ~~the~~ key ~~for decrypting the software module.~~

4. (Original) The installation module of claim 3, wherein the key is encrypted.

5. (Original) The installation module of claim 2, wherein the database includes a hash value for each of the trigger files.

6. (Original) The system of claim 1, wherein the encrypted software module is a cryptographic software module.

7. (Original) The system of claim 6, wherein the encrypted software module is a dynamic-link library (DLL) for providing a secure socket layer (SSL).

8. (Original) The system of claim 1, wherein the encrypted software module resides on a computer-readable medium.

9. (Currently amended) A software system comprising:
an installation module comprising:

an encrypted software module,

a decryption key, and

an executive for decrypting the encrypted software module with the decryption key when at least one of a set of trigger files is stored on a computing system, wherein each file of the set of trigger files indicates authorization to load the software module onto a computing system ~~does not include a key for decrypting the encrypted software module~~; and

a setup program for invoking the executive and loading the decrypted software module onto the ~~the~~ computing system.

10. (Original) The software system of claim 9, wherein the setup program loads one of the trigger files onto the computing system.

11. (Original) The software system of claim 10, wherein the setup program retrieves the loaded trigger file from an Internet website.

12. (Original) The software system of claim 9, wherein the encrypted software module is a cryptographic software module.

13. (Original) The software system of claim 12, wherein the encrypted software module is a dynamic-link library (DLL) for providing a secure socket layer (SSL).

14. (Original) The software system of claim 9, wherein the encrypted software module resides on a computer-readable medium.

15. (Currently amended) A computing method comprising:
decrypting an encrypted software module using a decryption key included with the encrypted software module when at least one of a set of trigger files is stored on a computing system, ~~wherein none of the trigger files includes a decryption key for decrypting the encrypted software module;~~ and
loading the decrypted software module onto the computing system.

16. (Original) The method of claim 15, wherein the decrypting step includes determining whether a prior version of the encrypted software module is stored on a computing system.

17. (Original) The method of claim 16, wherein the determining step includes retrieving hash values for the trigger files from a database.

18. (Currently amended) A computing method comprising:
decrypting an encrypted software module when at least one of a set of trigger files is stored on a computing system, wherein the decrypting includes retrieving a cryptographic key from a database of an installation module that includes the encrypted software module and using the retrieved key to decrypt the encrypted software module; and
loading the decrypted software module onto the computing system.

19. (Previously presented) The method of claim 15 and further including loading one of the trigger files onto the computing system.

20. (Original) The method of claim 19, wherein the loading step includes retrieving the loaded trigger file from an Internet website.

21. (Original) The method of claim 15, wherein the loading step includes loading a cryptographic software module.

22. (Original) The method of claim 15, wherein decrypting the encrypted software module includes retrieving the encrypted software module from a computer-readable medium.

23. (Original) A computer-readable medium having computer-executable instructions to cause a computing system to perform the method of claim 15.

24. (Previously presented) One or more computer-readable media having stored thereon a plurality of instructions that, when executed by one or more processors, cause the one or more processors to:

decrypt an encrypted software module when a trigger file is stored on a computing system, wherein the trigger file comprises a prior version of the encrypted software module; and

load the decrypted software module onto the computing system.

25. (Canceled).

26. (Previously presented) One or more computer-readable media as recited in claim 24, wherein the plurality of instructions further cause the one or more processors to load a different version of the software module onto the computing system when the trigger file is not stored on the computing system.

Claims 27-30. (Canceled)

31. (Previously presented) A method comprising:

checking whether at least one of a set of one or more trigger files is stored on a computer;

determining, based on the checking, which of multiple versions of a software module to install on the computer, wherein a first version of the multiple versions has greater than a threshold strength encryption, and wherein a second version of the multiple versions has not greater than the threshold strength encryption;

wherein the determining comprises determining that the first version is to be installed on the computer if at least one of the set of one or more trigger files is stored on the computer, and that the second version is to be installed on the computer if none of the set of one or more trigger files is stored on the computer;

wherein if the first version is to be installed on the computer then decrypting the first version and installing the decrypted first version; and

wherein if the second version is to be installed on the computer then installing the second version.

32. (Previously presented) A method as recited in claim 31, wherein the threshold strength encryption comprises 56-bit encryption.

33. (Previously presented) A method as recited in claim 31, wherein one of the set of one or more trigger files comprises a prior version of the software module.

34. (Canceled).

35. (New) The system of claim 1, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm.

36. (New) The installation module of claim 2, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm.
